Subscribe (Full Service) Register (Limited Service, Free) Login

Search: ● The ACM Digital Library ○ The Guide

THE ACM DIGITAL LIBRARY

Feedback

hash xor session key public key encrypt
Terms used: hash xor session key public key encrypt

Foı

Sort results by: relevance

Display results: expanded form

Save results to a Binder

□ Open results in a new window

Refine these results with Ad
Try this search in The ACM (

Results 1 - 20 of 35

Result page: 1 2 next >>

1 LIGER: implementing efficient hybrid security mechanisms for heterogeneous sensor networks
Patrick Traynor, Raju Kumar, Hussain Bin Saad, Guohong Cao, Thomas La Porta
June 2006 MobiSys '06: Proceedings of the 4th international conference on Mobile systems, applications and services
Publisher: ACM
Full text available: pdf(592.00 KB) Additional Information: full citation, abstract, references, index terms

Bibliometrics: Downloads (6 Weeks): 3, Downloads (12 Months): 154, Citation Count: 0

The majority of security schemes available for sensor networks assume deployment in areas without access to a wired infrastructure. More specifically, nodes in these networks are unable to leverage key distribution centers (KDCs) to assist them with ...

Keywords: heterogeneous sensor networks, hybrid network security, probabilistic authentication, probabilistic key management

2 Public-key cryptography and password protocols
Shai Halevi, Hugo Krawczyk
August 1999 ACM Transactions on Information and System Security (TISSEC), Volume 2 Issue 3
Publisher: ACM
Full text available: pdf(275.84 KB) Additional Information: full citation, abstract, references, cited by, index terms, review

Bibliometrics: Downloads (6 Weeks): 27, Downloads (12 Months): 319, Citation Count: 11

We study protocols for strong authentication and key exchange in asymmetric scenarios where the authentication server possesses ~a pair of private and public keys while the client has only a weak human-memorizable password as its authentication key. ...

Keywords: dictionary attacks, hand-held certificates, key exchange, passwords, public passwords, public-key protocols

3 A survey of key management for secure group communication
Sandro Rafaeli, David Hutchison
September 2003 ACM Computing Surveys (CSUR), Volume 35 Issue 3
Publisher: ACM

Full text available: pdf(346.27 KB) Additional Information: full citation, abstract, references, cited by, index terms

Bibliometrics: Downloads (6 Weeks): 51, Downloads (12 Months): 642, Citation Count: 15

Group communication can benefit from IP multicast to achieve scalable exchange of messages. However, there is a challenge of effectively controlling access to the transmitted data. IP multicast by itself does not provide any mechanisms for preventing ...

Keywords: Group Key Distribution, Multicast Security

4 Self-organised group key management for ad hoc networks

Ling Luo, Rei Safavi-Naini, Joonsang Baek, Willy Susilo
March 2006 ASIACCS '06: Proceedings of the 2006 ACM Symposium on Information, computer and communications security
Publisher: ACM

Full text available: pdf(430.32 KB) Additional Information: full citation, abstract, references, index terms

Bibliometrics: Downloads (6 Weeks): 13, Downloads (12 Months): 198, Citation Count: 0

We propose a fully distributed group key distribution protocol for ad hoc networks. The protocol uses a key pre-distribution step that is performed by each node independently and generates secure links between nodes in a neighbourhood. The key pre-distribution ...

Keywords: Ad hoc network, key distribution, privacy homomorphism

5 The dual receiver cryptosystem and its applications

Theodore Diament, Homin K. Lee, Angelos D. Keromytis, Moti Yung
October 2004 CCS '04: Proceedings of the 11th ACM conference on Computer and communications security
Publisher: ACM

Full text available: pdf(329.14 KB) Additional Information: full citation, abstract, references, cited by, index terms

Bibliometrics: Downloads (6 Weeks): 10, Downloads (12 Months): 55, Citation Count: 1

We put forth the notion of a dual receiver cryptosystem and implement it based on bilinear pairings over certain elliptic curve groups. The cryptosystem is simple and efficient yet powerful, as it solves two problems of practical importance whose solutions ...

Keywords: digital signature, elliptic curves, key escrow, pairing-based cryptography, public key, puzzles, useful secure computation

6 Nark: receiver-based multicast non-repudiation and key management

Bob Briscoe, Ian Fairman
November 1999 EC '99: Proceedings of the 1st ACM conference on Electronic commerce
Publisher: ACM

Full text available: pdf(168.86 KB) Additional Information: full citation, references, cited by, index terms

Bibliometrics: Downloads (6 Weeks): 5, Downloads (12 Months): 41, Citation Count: 2

Keywords: Internet, audit trail, key management, multicast, non-repudiation, smartcard, watermark

7 Key management for encrypted broadcast

Avishai Wool

May 2000 ACM Transactions on Information and System Security (TISSEC), Volume 3 Issue 2

Publisher: ACM

Full text available: pdf(220.36 KB) Additional Information: full citation, abstract, references, index terms

Bibliometrics: Downloads (6 Weeks): 5, Downloads (12 Months): 118, Citation Count: 0

We consider broadcast applications where the transmissions need to be encrypted, such as direct broadcast digital TV networks or Internet multicast. In these applications the number of encrypted TV programs may be very large, but the secure memory capacity ...

Keywords: conditional access, pay-per-view

8 Key-assignment strategies for CPPM

André Adelsbach, Jörg Schwenk

September 2004 MM&Sec '04: Proceedings of the 2004 workshop on Multimedia and security

Publisher: ACM

Full text available: pdf(454.53 KB) Additional Information: full citation, abstract, references, index terms

Bibliometrics: Downloads (6 Weeks): 4, Downloads (12 Months): 37, Citation Count: 0

CSS, the first system to protect multimedia content on the new DVD medium failed badly, because both its encryption algorithm and its key management could easily be broken. A new industry initiative, the 4C Entity, LLC (founded by IBM, Intel, Matsushita ...

Keywords: CPPM, content protection, device revocation, key-assignment, key-management

9 Analyzing security protocols with secrecy types and logic programs

Martín Abadi, Bruno Blanchet

January 2005 Journal of the ACM (JACM), Volume 52 Issue 1

Publisher: ACM

Full text available: pdf(438.64 KB) Additional Information: full citation, abstract, references, cited by, index terms, review

Bibliometrics: Downloads (6 Weeks): 15, Downloads (12 Months): 175, Citation Count: 8

We study and further develop two language-based techniques for analyzing security protocols. One is based on a typed process calculus; the other, on untyped logic programs. Both focus on secrecy properties. We contribute to these two techniques, in particular ...

Keywords: Cryptographic protocols, logic programming, process calculi, secrecy properties, typing

10 A user-centric anonymous authorisation framework in e-commerce environment

Richard Au, Harikrishna Vasanta, Kim-Kwang Raymond Choo, Mark Looi

March 2004 ICEC '04: Proceedings of the 6th international conference on Electronic commerce

Publisher: ACM

Full text available: pdf(291.06 KB) Additional Information: full citation, abstract, references, cited by

Bibliometrics: Downloads (6 Weeks): 16, Downloads (12 Months): 86, Citation Count: 1

A novel user-centric authorisation framework suitable for e-commerce in an open environment is proposed. The credential-based approach allows a user to gain access rights anonymously from various service providers who may not have pre-existing relationships. ...

11 Anti-vamming trust enforcement in peer-to-peer VoIP networks
Nilanjan Banerjee, Samir Saklikar, Subir Saha
July 2006 IWCMC '06: Proceedings of the 2006 international conference on Wireless communications and mobile computing
Publisher: ACM
Full text available: pdf(377.95 KB) Additional Information: full citation, abstract, references, index terms

Bibliometrics: Downloads (6 Weeks): 15, Downloads (12 Months): 236, Citation Count: 0

With the increasing popularity of Voice over IP (VoIP) the threat of "vamming" or VoIP spam calls is looming large over the telecom industry. This threat arises out of the "openness" of the IP-based network such as the Internet, which enables anyone ...

Keywords: identity, peer-to-peer networks, trust, vamming, voice over IP

12 A secure and private system for subscription-based remote services
Pino Persiano, Ivan Visconti
November 2003 ACM Transactions on Information and System Security (TISSEC), Volume 6 Issue 4
Publisher: ACM
Full text available: pdf(241.65 KB) Additional Information: full citation, abstract, references, cited by, index terms

Bibliometrics: Downloads (6 Weeks): 6, Downloads (12 Months): 112, Citation Count: 2

In this paper we study privacy issues regarding the use of the SSL/TLS protocol and X.509 certificates. Our main attention is placed on subscription-based remote services (e.g., subscription to newspapers and databases) where the service manager charges ...

Keywords: Access control, anonymity, cryptographic algorithms and protocols, privacy, world-wide web

13 Methods and limitations of security policy reconciliation
Patrick McDaniel, Atul Prakash
August 2006 ACM Transactions on Information and System Security (TISSEC), Volume 9 Issue 3
Publisher: ACM
Full text available: pdf(621.63 KB) Additional Information: full citation, abstract, references, index terms

Bibliometrics: Downloads (6 Weeks): 22, Downloads (12 Months): 236, Citation Count: 0

A security policy specifies session participant requirements. However, existing frameworks provide limited facilities for the automated reconciliation of participant policies. This paper considers the limits and methods of reconciliation in a general-purpose ...

Keywords: Security policy

14 Application of synchronous dynamic encryption system (SDES) in wireless sensor networks
Hamdy S. Soliman, Mohammed Omari
October 2005 PE-WASUN '05: Proceedings of the 2nd ACM international workshop on Performance evaluation of wireless ad hoc, sensor, and ubiquitous networks
Publisher: ACM
Full text available: pdf(59.63 KB) Additional Information: full citation, abstract, references, index terms

Bibliometrics: Downloads (6 Weeks): 5, Downloads (12 Months): 122, Citation Count: 0

In this paper, we introduce a novel security protocol for wireless network of sensors. The new security mechanism is efficient, flexible, and very amenable for deployment in the resource constrained sensor networks. Our cryptosystem is a simple and fast ...

Keywords: deployment knowledge, encryption permutation vectors, power balancing, sensors security primitives, stream ciphers

15 Architectural Support for High Speed Protection of Memory Integrity and Confidentiality in Multiprocessor Systems
Weidong Shi, Hsien-Hsin S. Lee, Mrinmoy Ghosh, Chenghuai Lu
September 2004 PACT '04: Proceedings of the 13th International Conference on Parallel Architectures and Compilation Techniques
Publisher: IEEE Computer Society
Full text available: pdf(255.33 KB) Additional Information: full citation, abstract, references, cited by

Bibliometrics: Downloads (6 Weeks): 6, Downloads (12 Months): 43, Citation Count: 3

Recently there is a growing effort in both the architecture and the security community to create a hardware solution for authenticating system memory.As shown in the previous work, hardware-based memory authentication will become a vital component for ...

16 A survey of cryptographic primitives and implementations for hardware-constrained sensor network nodes
Rodrigo Roman, Cristina Alcaraz, Javier Lopez
August 2007 Mobile Networks and Applications, Volume 12 Issue 4
Publisher: ACM
Full text available: pdf(468.79 KB) Additional Information: full citation, abstract, references, index terms

Bibliometrics: Downloads (6 Weeks): 46, Downloads (12 Months): 237, Citation Count: 0

In a wireless sensor network environment, a sensor node is extremely constrained in terms of hardware due to factors such as maximizing lifetime and minimizing physical size and overall cost. Nevertheless, these nodes must be able to run cryptographic ...

Keywords: cryptography, hardware, sensor networks

17 Robust, anonymous RFID authentication with constant key-lookup
Mike Burmester, Breno de Medeiros, Rossana Motta
March 2008 ASIACCS '08: Proceedings of the 2008 ACM symposium on Information, computer and communications security
Publisher: ACM
Full text available: pdf(315.43 KB) Additional Information: full citation, abstract, references, index terms

Bibliometrics: Downloads (6 Weeks): 0, Downloads (12 Months): 0, Citation Count: 0

A considerable number of anonymous RFID authentication schemes have been proposed. However, current proposals either do not provide robust security guarantees, or suffer from scalability issues when the number of tags issued by the system is very large. ...

Keywords: RFID, availability, privacy, provably secure protocols, scalability, unlinkability

18 Graceful service degradation (or, how to know your payment is late)
Alexandr Andoni, Jessica Staddon
June 2005 EC '05: Proceedings of the 6th ACM conference on Electronic commerce
Publisher: ACM
Full text available: pdf(275.69 KB) Additional Information: full citation, abstract, references, index terms

Bibliometrics: Downloads (6 Weeks): 2, Downloads (12 Months): 19, Citation Count: 0

When distributing digital content over a broadcast channel it's often necessary to *revoke* users whose access privileges have expired, thus preventing them from recovering the content. This works well when users make a conscious decision to leave ...

Keywords: broadcast encryption, copyright protection, degradation scheme, moderately-hard functions, revocation scheme

19 Analyzing security protocols with secrecy types and logic programs
Martín Abadi, Bruno Blanchet
January 2002 ACM SIGPLAN Notices, Volume 37 Issue 1
Publisher: ACM
Full text available: pdf(189.62 KB) Additional Information: full citation, abstract, references, cited by

Bibliometrics: Downloads (6 Weeks): 6, Downloads (12 Months): 33, Citation Count: 8

We study and further develop two language-based techniques for analyzing security protocols. One is based on a typed process calculus; the other, on untyped logic programs. Both focus on secrecy properties. We contribute to these two techniques, in particular ...

20 Analyzing security protocols with secrecy types and logic programs
Martín Abadi, Bruno Blanchet
January 2002 POPL '02: Proceedings of the 29th ACM SIGPLAN-SIGACT symposium on Principles of programming languages
Publisher: ACM
Full text available: pdf(189.62 KB) Additional Information: full citation, abstract, references, cited by

Bibliometrics: Downloads (6 Weeks): 6, Downloads (12 Months): 33, Citation Count: 8

We study and further develop two language-based techniques for analyzing security protocols. One is based on a typed process calculus; the other, on untyped logic programs. Both focus on secrecy properties. We contribute to these two techniques, in particular ...

Results 1 - 20 of 35 Result page: 1 2 next >>

Useful downloads: Adobe Acrobat QuickTime Windows Media Player Real Player